APRIL 2021

rma®
THE RISK MANAGEMENT ASSOCIATION

THIRD-PARTY CONCENTRATION RISK

Enterprise Risk • Credit Risk • Market Risk • Operational Risk • Regulatory Affairs • Securities Lending • Internal Audit

Every firm in every sector operates within a complex extended enterprise, with extensive reliance on third-, fourth-, and nth party relationships. Concentration risk is emerging as a top-line risk and an increasing area of focus for many senior executives and risk professionals. There are many forms of concentration risk, some of which are predominant in third-party risk management that will be addressed in this RMA Third-Party Risk Management (3PRM) Round Table members' whitepaper.

Most firms have limited risk insight about third-party risk management capabilities implemented by their critical third parties. This deficiency results in inadequate information, risk identification, and management of material fourth and fifth parties. This affects your firm's ability to manage concentration risk because information about material fourth and fifth parties, including services delivered, service delivery location, etc. will not be made available to you.

In this document, senior level third-party risk management practitioners and subject matter experts—members of RMA's Third-Party Risk Management Round Table—will share their expertise and insight into current best practices for identifying and treating third- and fourth-party concentration risk. The level of detail found in this whitepaper makes this an ideal tool for third-party and operational risk management professionals, and business owners in the first line of defense.

Many thanks to:

- Cheryl Dimitroff, Senior Strategist, Third-Party Management, KeyBank NA
- Yatin Patel, Associate Director, Third-Party Standards and Advisory, Royal Bank of Canada
- Christe Smith, Director, Third-Party Risk, Bank OZK
- Natalia Weems, AVP Vendor Management, Dollar Bank
- Linda Tuck Chapman, CEO, Third-Party Risk Institute Ltd. (Working Group Chair)
- Sylwia Czajkowska, Associate Director, Operational Risk, RMA

In this document we present third- and fourth-party concentration risk exposure as a series of "Problem Statements" regarding:

- Inventory Management.
- Entity/Activity.
- Geographic/Geopolitical.
- Cloud.
- Fourth Party.
- Systemic.

Leveraging their expertise and experience, the working group makes specific, actionable recommendations to mitigate or treat each type of concentration risk. At the conclusion of these recommendations, this paper provides sample metrics that can inform development of actionable KRIs to manage third-party concentration risk.

INVENTORY MANAGEMENT

Problem Statement #1:

Many firms don't have a complete inventory of third-party relationships, particularly for non-vendor third-parties and material fourth-parties. There is increasing awareness of the need to know who you're doing business with, what services they are delivering or supporting, the service delivery location, and the types and amount of risk they expose your firm to (e.g., access to your firm's networks, systems, and data).

Description:

If you don't have a complete inventory of critical third-party relationships and material fourth-party relationships, you will have an incomplete view of concentration risks.

Recommendations:

1. Develop and execute a plan to create a complete inventory of in-scope third-party relationships.
2. Create a centralized data source by recording these in your third-party risk management platform/software.
3. Strengthen risk insight by including key data elements in your inventory (e.g., services, service delivery location, material fourth-parties).
4. Examine capture and onboarding processes and controls to ensure business segments can't engage third-parties outside of your policy (e.g., implement controls in General Counsel's Office, accounts payable, cybersecurity).
5. Periodically reconcile accounts ayable, contracts, and third-party databases. (AI capabilities can minimize work effort.)
6. Strengthen processes to identify use of cloud computing by third- and fourth-parties, particularly where cloud solutions are interacting with each other.

THERE IS INCREASING AWARENESS OF THE NEED TO KNOW WHO YOU'RE DOING BUSINESS WITH, WHAT SERVICES THEY ARE DELIVERING OR SUPPORTING, THE SERVICE DELIVERY LOCATION, AND **THE TYPES AND AMOUNT OF RISK THEY EXPOSE YOUR FIRM TO.**

ENTITY AND ACTIVITY CONCENTRATION RISK

Problem Statement #2:

Many firms do not have a formal process in place to adequately identify and manage entity and activity concentration risk and are therefore unable to provide transparency to senior management. Entity concentration risk is amplified when a critical third party is also a material fourth party.

Description:

Entity concentration risk results when you place heavy reliance on a single third- or fourth-party to support your organization. This occurs when a single third party performs multiple services, a high volume of work, or more than one critical activity. Entity concentration risk may also be caused by fourth-party usage when multiple third-parties rely on the same fourth-party provider (e.g., cloud providers, data centers).

Excessive reliance on a particular third- or fourth-party can leave your company vulnerable when incidents occur or a transition from a third-party is necessary. It can lead to interrupted operations, overpayment for services, monetary and reputational losses, and other adversities.

Recommendations:

1. Identify which activities are performed by each third party, andnote which of these are critical to the business owner or the enterprise.
2. Collaborate with risk experts and subject matter experts to establish KRIs and thresholds that determine when entity concentration risk is misaligned with your company's risk appetite. Consider having KRIs and thresholds approved by senior management.
3. During due diligence, consider the impact of new contracts and statements of work on entity concentration risk KRIs and thresholds. Challenge as appropriate, and include this information in risk acceptance documentation.
4. Periodically (annually) assess entity concentration risk at the a) single entity level; b) portfolio level (aggregate risk across the in-scope population); and c) line of business level.
5. Develop quarterly and annual reporting to provide transparency to senior management that includes risk, assessment, and performance results for affected third parties.
6. Determine what additional monitoring or assessment activity(ies) should take place when entity concentration risk is identified.
7. Decide on the threshold for when mitigating the risk is necessary (e.g., transitioning to another third-party, bringing the service in house, dispersing volume to other providers).
8. (RoadMap item) Determine how to treat the risk of material fourth-parties that cause higher levels of entity concentration risk.

GEOGRAPHIC CONCENTRATION RISK

Problem Statement #3:

Geographic concentrations can arise when a firm's internal operations, and/or its third- and fourth-parties are located in the same region or are dependent on the same power or telecommunications physical infrastructure.

Description:

Some geographic regions were severely impacted, resulting in significant disruption in service delivery. If both a financial firm or many of its critical third- and fourth-parties are located in the same region, there is a risk that a natural disaster or other serious risk event may have a material impact on all parties.

Recommendations:

1. Appoint one individual responsible for understanding and keeping abreast of the region with concentration risk.
2. Include geographic concentration risk as part of the due diligence and on-boarding process such that line of business executives and risk committees understand the risk and the exposure if a decision is made to move forward.
3. Expand the scope of third-party inventory and records by implementing a questionnaire that requests the third-party to provide current and accurate information on the following:
    a. Location of corporate headquarters, service delivery locations, data center(s), backup site(s), and other critical locations (data storage, help desk, contact center).
    b. Location of all material fourth-parties and essential contractors, capturing the same information as for third-parties.
    c. Significant control deficiencies, issues, and incidents for critical third- and material fourth-parties.
4. Assess the impact if a region is not able to deliver services.
5. Consider geo-mapping this information to create a visual record. There are several no-cost tools available.
6. When developing risk mitigation strategies, consider:
    a. Implementing a multi-region/third-party sourcing strategy.
    b. Requiring existing third-parties to provide services from a different facility.
    c. Sourcing other third-parties with operations in different regions.
    d. Maintaining in-house staff that can handle the most important activities.
7. Establish solid contract provisions for notification and approval requirements to maintain control over geographic concentration risk.
    a. When negotiating or renewing the contract, include a requirement for the highest-criticality relationships and (where known) those in areas with higher geographic concentration risk to provide a copy of their disaster recovery/business continuity (DR/BCP) plans (full, partial, highlights), results of testing, and financial statements on an annual basis.
    b. When negotiating or renewing the contract, include a requirement for relationships with a short recovery time objective (RTO) that are delivering services from areas with higher geographic concentration risk to provide a copy of their DR/BCP plans (full, partial, highlights), results of testing, and financial statements on an annual basis.
    c. Require that critical third parties attest that they hold their material fourth-parties to the same requirements and standards and have a similar level of risk insight. Implementation may require changes to due diligence and contracting practices.

8. Analysis and risk identification:
    a. Define the geographic reach(es) for the analysis (e.g., within a city, a 75-mile radius, a region, or a country).
    b. Identify the areas with the highest number of "hits" (your operations + third-party + fourth-party).
    c. For areas with high geographic concentration risk, determine what the exposure is (e.g., high volumes of data; core services; critical processing centers, city/region, country).
    d. Triage results of analysis to identify highest source(s) of geographic risk. Ensure third- and fourth-parties with high geographic concentration risk are included in business impact analysis (BIA).
    e. Analyze sources of higher levels of geographic concentration risk to identify opportunities to reduce it by relocating services to alternate locations or backup centers.
9. Increase monitoring requirements and/or require relationship managers to attest that they are monitoring incidents and risk events. Monitor news for and during serious risk events, with a geo-mapping overlay.
10. Establish KRIs and thresholds for in-scope concentration risks. Review the existing portfolio periodically to identify engagements that meet geographic concentration risk triggers.
11. Periodically assess the feasibility of reducing geographic concentration risk.
12. Periodically report to senior management on geographic concentration risk items (e.g., specific concentrations, risk events and impact, KRIs and results, higher risk exposure relationships due to controls deficiencies, weak financial condition, and negative news).

Country risk and geopolitical risk are inseparable. Country and geopolitical risks should be considered when identifying and treating geographic concentration risk. All higher levels of country and geopolitical risk should be treated as part of geographic concentration risk.

Recommendations:

1. Maintain the inventory of the third- and fourth-party relationships, including headquarters and service delivery locations.
2. Conduct a thorough geopolitical analysis for any third- or fourth-parties proposed for or located in a high geopolitical risk country or region. Consider:
    a. Geography – access and weather.
    b. Political – stability of the government and the economy, history of nationalizing businesses, and other "unfriendly" practices.
    c. Regulatory environment – regulators, regulations, and history of enforcement actions.
    d. Infrastructure – condition of essential infrastructure, reliability (roads, power, telecom).
    e. Crime Rate – safety and security considerations.
    f. Availability of a skilled workforce – volume and sources of skilled labor, education, employment laws, and impact on obligations and costs.
    g. Culture – impact of culture on operational expectations.
    h. ESG – laws and track record.
    i. Region – track record, amount of investment capital, and success rates for similar businesses.

CLOUD CONCENTRATION

Problem Statement #4:

Cloud concentration risk for most firms is high, given the limited number of cloud service providers and the pervasive use of the same cloud provider as well as multiple different clouds interacting to supply a third-party product or service.

Description:

Third-party products and services have become increasingly more complex, along with the need for increased agility and elasticity. Many third-party solutions interact between business segments, and involve large, multifaceted third-party outsourcing relationships and many material fourth-parties and cloud solutions (e.g., payment, settlement, and clearing systems). An added layer of complexity is when these ecosystems also interact with one another, creating aggregated concentration risk and cloud interconnectedness.

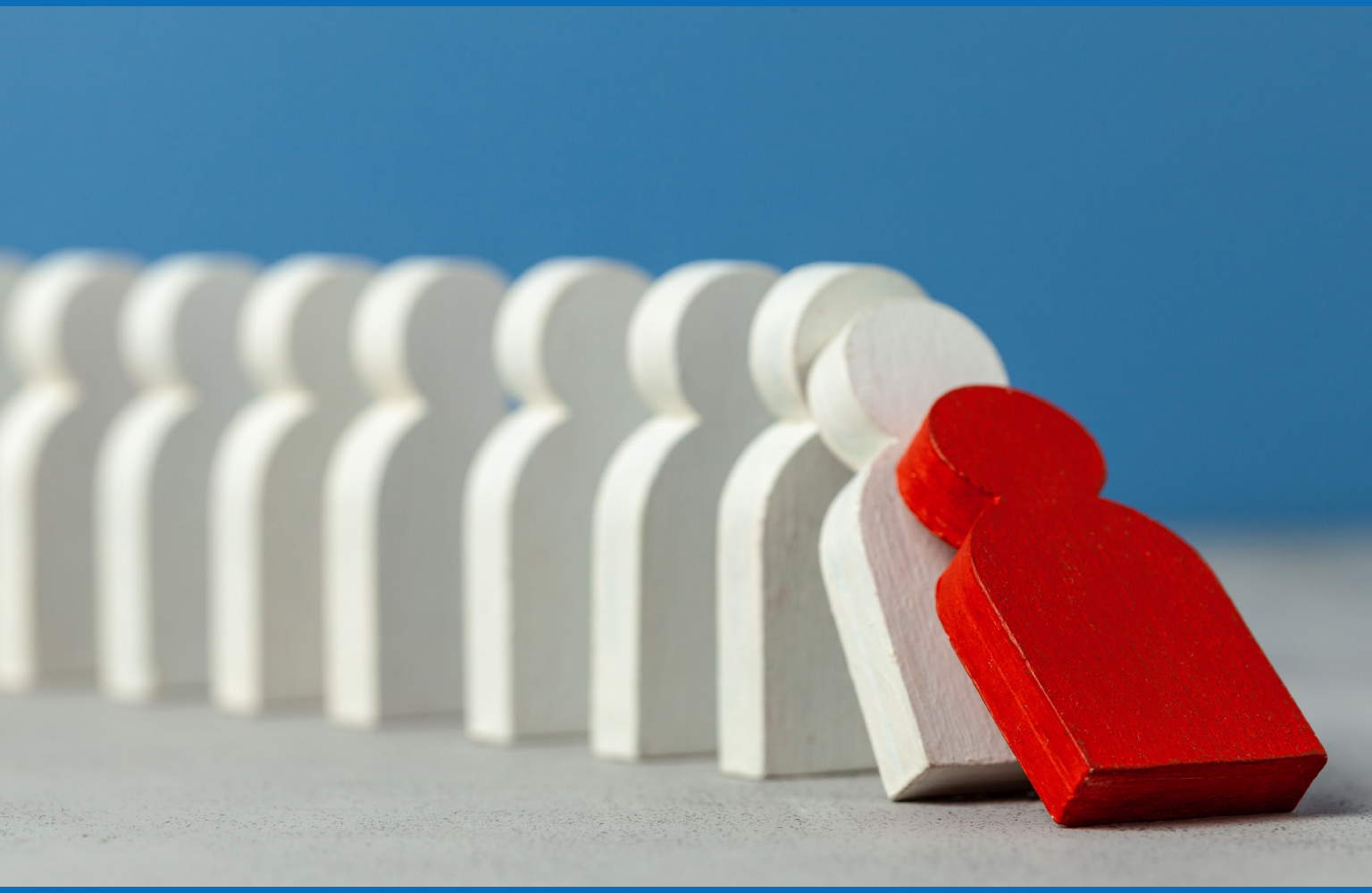
It is noted that financial services regulators do not include any cloud service providers in the list of 200 fintechs they examine, despite the significant systemic risk they bring to the sector.

Recommendations:

1. Identify all third- and fourth-party cloud providers supporting your firm.
2. Maintain an aggregated inventory of all third- and fourth-party cloud solutions, and which systems, products, services, and data they access. Ideally, identify nth parties where possible and approved locations of servers utilized for your firm.
3. Diversify cloud providers to the extent possible.
4. Minimize the risk of outages and high volumes of data with one provider. Consider engaging third parties who have mitigated this risk by utilizing multiple cloud solutions.
5. Establish solid contract provisions including (1) clear exit strategies, (2) requirements for data destruction in all locations, (3) clear cache(s) when exiting a cloud solution, (4) due diligence/auditability rights, (5) strong information security requirements, (6) requirements including notifications for fourth-party cloud solutions, (7) security requirements for APIs (application programming interfaces), (8) data storage restrictions, by country, (9) specific recovery priority order, aligned with the line of business required RTO.
6. Map your predominant cloud providers to your firm's products and services to identify another layer of cloud concentration risk.
7. Consider identifying complex relationships with interconnected data centers and cloud providers to identify higher levels of aggregated risk.
8. Consider the impact of a serious event or insolvency of a cloud solution on the broader enterprise.
9. Understand the cross-border, cross-jurisdictional risks of cloud solutions, including interactions between multiple cloud solutions.
10. Ensure enterprise data strategies include third-party data storage, management, protection, and destruction requirements.

FINANCIAL SERVICES REGULATORS DO NOT INCLUDE ANY CLOUD SERVICE PROVIDERS IN THE LIST OF 200 FINTECHS THEY EXAMINE, DESPITE THE SIGNIFICANT SYSTEMIC RISK THEY BRING TO THE SECTOR.

FOURTH-PARTY CONCENTRATION RISK



Problem Statement #5:

There are currently few best practices for assessing and addressing fourth-party concentration risk. Fourth-party concentration risk arises when multiple third parties are using the same fourth-party. If the concentration risk is with one or more key fourth-parties, it may impact multiple third parties. This cascade effect may impact one or more of your business segments.

Your critical third-party may be exposed to a high level of single entity concentration risk because they have outsourced most or all of a core process to a single fourth-party. In this instance your firm has a high level of fourth-party concentration risk. Though not always transparent, this represents a higher level of third-party risk than today's standard risk identification processes would identify. If either the third-party or the fourth-party fails to perform, the financial firm may be forced into its contingency plan for the affected process or processes.

Identifying fourth-party concentration risk can only be done if the right data is available. By excluding fourth-parties from your analysis, there is the potential to understate concentration risk. For example, your firm may be using the same company as a third and a fourth-party across many engagements (e.g., Amazon, Google, etc.) Avoiding or reducing fourth-party concentration through diversification may not be an option. This is because your firm is not contracted with the fourth-party.

Description:

Not all fourth-parties are equal. Define what a material fourth-party is, why it is significant, and what data you need. Your relationship with material fourth-parties is at arm's length, at best. Because of this, sound data collection practices and data quality are key. SolarWinds is an excellent but chilling example of fourth- and fifth-party risk and the impact of deficient third-party risk management capabilities by your firm's critical third-parties.

Recommendations:

1. In collaboration with risk professionals and legal, create a standard definition of "material" fourth-parties for inclusion in due diligence questionnaire(s) and contracts.
2. Determine criteria (scope) for requiring third-parties to complete due diligence about (1) their third-party risk management capabilities, and (2) to provide information about their material fourth-parties. Avoid free-form fields that can impair data analysis.
3. During due diligence assess the third-parties lifecycle management capabilities for critical third-parties and material fourth-parties.
4. Consider developing a sub-program to assess the existence and operational effectiveness of third-party management capabilities for material fourth-parties, and required documentary evidence (consider including in your future state Roadmap).
5. Before awarding a contract to a third-party, consider the impact of their material fourth-parties on your firm's concentration risk thresholds.
6. An emerging risk management activity is to determine whether any material fourth-parties represent a "single point of failure" due to high levels of operational dependency by your firm's critical third-parties; have access to sensitive or protected information, networks, and systems; or perform compliance activities/regulatory reporting on behalf of your firm.
7. [Semi]annual verification of information about material fourth-parties.
8. Strengthen contract controls (e.g., [semi]-annual confirmation of authorized material fourth-parties, notification and pre-approval of changes, any restrictions, and limitations).
9. Expand the scope of concentration risk analysis and set concentration risk thresholds to encompass both critical third- and material fourth-parties.

Remember that if your firm is already contracted with a material fourth-party as its third-party, you're already risk-informed.

SYSTEMIC CONCENTRATION RISK

Problem Statement #6:

Risk insight into pervasively utilized service providers, otherwise known as systemic concentration risk, is largely unavailable.

Description:

Many financial firms utilize the same third- or n^{th} parties for various reasons including best in class and single service provider. There is a direct connection between systemic concentration and the potential for high-risk losses.

Third-parties falling into this systemic concentration risk category are potential single points of failure whose unavailability or failure have the potential to disrupt the financial industry.

Recommendations:

1. Identify a qualified relationship manager who accepts their responsibility to oversee each relationship and accepts accountability for managing the relationship and monitoring the risks.
2. Maintain an aggregated inventory of all critical third and material fourth-parties; which systems, products, services, and data they access; and the service delivery location. Ideally identify n^{th} parties, where possible.
3. Diversify third-parties, and consider the impact on concentration risk presented by their n_{th} parties, where possible.
4. Consider and quantify the impact (firm and customers) should a systemic provider be unavailable.
5. Contract for a specific recovery priority order, aligned with the line of business required RTO.

Many firms have not yet developed KRIs for third- and fourth-party concentration risk. Many thanks to executives in the sector—members of RMA's Third-Party Risk Management Round Table—for their responses to RMA's KRI survey and their contributions to this whitepaper, including those that advised that their institution has not implemented KRIs for concentration risk. For confidentiality, the institutions and executives are not identified here.

IDENTIFY A QUALIFIED RELATIONSHIP MANAGER WHO ACCEPTS THEIR RESPONSIBILITY **TO OVERSEE EACH RELATIONSHIP AND ACCEPTS ACCOUNTABILITY** FOR MANAGING THE RELATIONSHIP AND MONITORING THE RISKS.

KEY RISK INDICATORS (KRIs) AND THRESHOLDS

#	Name	Description	Metrics
1	Supplier Process Concentration Risk	The indicator identifies a unique count of suppliers providing services to a critical process (Criticality Level) and that are material. The value calculated based on unique counts for each process drives a score that goes into an overall status calculation. The lower the concentration, the lower the score.	20+ for Red
2	Supplier Overall Concentration Risk	Supplier performs 2 or more critical processes (as defined by BCM) with annual spend >$500,000; Supplier has top 10 spend within the LOB and performs a critical process; Supplier has more than 20% or more of an Operating Groups spend and performs at least 1 critical process.	In process
3	Entity	5 or more managed engagements per TP More than 1 critical engagement with any third-party	Number of individual engagements per Third-Party Number of critical activities performed by one Third-Party
4	Entity	Percentage of high-risk contracts contracted to the legal entity	10%
5	Entity	Number of active products/service engagements per third-party for top 3 third parties across the enterprise	Top 3
6	Entity	Each third-party is assigned a tier based on the various risks that they bring to the relationship. Using an internally developed risk scoring model we generate a tier from 1-4. While we use this to help manage/prioritize third-party risk, it's not something that is used to manage concentration risk.	N/A

#	Name	Description	Metrics
7	Entity	1. Number and risk rating of services with entities. 2. Number and risk rating of services with Critical and High entities. ***3. Concentration of entities to a single service category.***	Exposure of services to a single entity. Exposure of services to critical and high-risk entities. Exposure of entities to a specific service category.
8	Activity	While we collect data about the services that each third-party is providing and whether it's the only provider of this service to our firm, we don't use it to measure or monitor concentration risk. We currently are more apt to manage this as a "category strategy" or "sourcing strategy" within first line Procurement rather than second line TPRM.	N/A
10	Activity	% of service outsourced to a specific third-party	> 50% of a particular service outsourced to one third-party.
11	Activity	1. Concentrations of services to a single Engagement Manager. 2. Concentrations of services to In-active Engagement Manager. 3. Concentrations of services to a single service category.	Increase/decrease over a period of time. Increase/decrease exposure of services to in-active engagement managers. Increase/decrease exposure to a specific service category.
12	Entity/activity	Evaluates concentrations for engagements by entity; Multi-business line support; risk severity.	Not provided

Country/Geographic/Geopolitical Concentration Risk

#	Name	Description	Metrics
1	Geographic/ Country	Production locations Material Subcontractor locations Recovery locations	>5 critical and/or high-risk production/material subcontractor locations within 75-mile radius >5 critical and/or high-risk recovery locations within 75-mile radius
2	Geographic/ Country	We perform a separate country risk analysis; Concentration risk in a particular country would be identified with the KRI above	N/A
3	Geographic/ Country	Includes geopolitical locations trending for higher risk; Third-party locations supporting bank business	Not provided
4	Geographic	Percentage of high-risk contracts owned by the group, concentrated on a single geographical area outside country for bank's head office.	10%
5	Geographic/ Country	While we collect geographic information for third and fourth parties, but the data is not currently used to manage concentration risk within TPRM (side note - that risk is surfaced within the "country risk" function of the bank). Internal function scores are used to forecast the geopolitical environment for countries where we have third-party vendors. Anything that indicates a "high" risk requires additional review during the contracting process, but we do not incorporate it into our concentration risk metric.	N/A
6	Geographic/ Country	1. Inherent Risk distribution by Country of Service Origination 2. Concentrations in countries outside of the U.S. and along risk levels	Exposure to a specific country Exposure of Entities to changing regional risk landscape.

Fourth-Party Concentration Risk

#	Name	Description	Metrics
1	Material Subcontrac-tors	Production locations Material Subcontractor locations Recovery locations	3 or more high-risk TPs with the same material subcontractor • See Entity above
2	Subcontrac-tor	Trending for subcontractor support across higher risk engagements.	Not provided
3	3rd and 4th Party	Critical services by third-party LOBS using these services Critical processes that use these services Third parties also using our third party (4th parties)	Internal scoring model ranked using High, Medium, Low (restrictions on us-age of High based on review/approval)
4	3rd and 4th Party	1. Concentration of entities along risk levels where an entity is both 3rd and 4th party. 2. 4th Party concentration along risk levels.	Exposure to top 20 entities Exposure of a specific 4th Party in a risk stripe.

Cloud Concentration Risk

#	Name	Description	Metrics
1	Cloud	Included with 4th party	No separate KRIs at this time
2	Cloud	Included as part of third- and fourth-party concentra-tion risk factors/trending	N/A
3	Cloud	High-risk contracts outsourced to the CSP	Percentage of high-risk contracts out-sourced to the CSP (under review)
4	Cloud	While we collect data related to cloud usage across our third- and fourth-party populations, the data is not currently used to measure or monitor concentration risk.	N/A
5	Cloud	1. 3rd vs. 4th party public cloud concentration 2. Cloud concentration by business line 3. Public Cloud concentration along risk lines 4. Public Cloud concentration along risk lines and data sensitivity	Exposure to 3rd vs. 4th party public cloud Exposure of a business line Exposure along risk lines Exposure along data sensitivity

This is a small sample but represents a significant change in recent years. Until recently, few financial firms had implemented third-party concentration risk KRIs and risk thresholds.

REFERENCES

Linda Tuck Chapman: "Third Party Risk Management: Driving Enterprise Value," published by RMA and for members at rmahq.org and Amazon.com

OCC Bulletin 2013-29: https://www.occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html

"Concentrations may arise when a bank relies on a single third-party for multiple activities, particularly when several of the activities are critical to bank operations."

Evaluate whether additional concentration-related risks may arise from the third-party's reliance on subcontractors and, if necessary, conduct similar due diligence on the third-party's critical subcontractors

Federal Reserve Board SR 13-19: https://www.federalreserve.gov/supervisionreg/srletters/sr1319.htm

"Concentration Risks arise when outsourced services or products are provided by a limited number of service providers or are concentrated in limited geographic locations."

FFIEC Strengthening the Resilience of Outsourced Technology Providers
https://ithandbook.ffiec.gov/1133

FFIEC IT Examination Handbook:
https://ithandbook.ffiec.gov/it-booklets/management/iii-it-risk-management/iiic-risk-mitigation/iiic8-third-party-management.aspx

FFIEC Appendix J:

"An increasing Concentration Risk corresponds to financial firms' increased use of third-party service providers; given the increased concentration of providers in the TSP industry, a financial firm should ensure that it has identified, and potentially prearranged, a comprehensive set of alternative resources to provide full resilience of operations in such scenarios."

FIL 44-2008:
https://www.fdic.gov/news/financial-firm-letters/2008/fil08044a.pdf

FDIC Consumer Compliance Examination Manual June 2019
https://www.fdic.gov/regulations/compliance/manual/7/VII-4.1.pdf

Consider keeping this document on hand as a quick reference for proven recommendations to identify and treat third-party concentration risk.

Please send your comments or requests for additional information to Linda Tuck Chapman: linda@3PRIinstitute.com

JOIN. ENGAGE. LEAD.

About RMA

The Risk Management Association (RMA) has been at the forefront of the development of the operational risk discipline in financial institutions since 2003.

The definition of operational risk is: *the risk of loss resulting from inadequate or failed internal processes, people, and systems, or from external events, but is better viewed as the risk arising from the execution of an institution's business functions.* Operational risk exists in every organization, regardless of size or complexity, from the largest institutions to regional and community banks.

For much of the past decade, the industry has been focused on measuring operational risk losses for capital allocation purposes, but in recent years has increased the focus on the process of managing operational risk.

RMA serves operational risk practitioners in large financial institutions, as well as regional, mid-tier, and community banks, at both the corporate level and the business line. RMA provides peer sharing, professional development and networking opportunities for our members through discussion groups, conferences, round tables, forums, courses, webinars, publications, and podcasts.

RMA also conducts surveys, benchmarking studies, and range-of-practice papers. In addition, RMA's Advanced Operational Risk Group shares industry views on aspects of AMA implementation with the U.S. financial services regulatory agencies toward a goal of successful AMA implementation. *The RMA Journal®* also regularly carries articles on operational risk topics.

RMA's operational risk activities are driven by the Operational Risk Council, whose mission is to promote sound practices in the management of operational risk in financial service institutions worldwide. It promotes understanding of the causes, events, and effects of operational risk through dissemination of management methods, sound practice tools, and materials. The Operational Risk Council is focused on the needs, challenges, and opportunities of all member institutions, including community, mid-tier, regional, and large banks, as well as non-bank financial institutions.

Major issue(s)/risk(s) within the market are listed below. COVID-19 has amplified all them:

- Technology
- Cybersecurity
- Information Security
- Third-Party Risk
- Fraud
- Succession/Talent challenges
- Challenge of returning to work
- Challenge of the possibility of second major outbreak
- Reputational risk in the event of second major outbreak

To learn more about RMA or our operational risk thought leadership pieces, contact Sylwia Czajkowska at sczajkowska@rmahq.org.